METHODS AND APPARATUS FOR PROVIDING SECURE TWO-PARTY PUBLIC KEY CRYPTOSYSTEM

Abstract

Techniques for an efficient and provably secure protocol by which two parties, each holding a share of a Cramer-Shoup private key, can jointly decrypt a ciphertext, but such that neither party can decrypt a ciphertext alone. In an illustrative embodiment, the secure protocol may use homomorphic encryptions of partial Cramer-Shoup decryption subcomputations, and three-move Σ-protocols for proving consistency.